모바일 보안 관리 기술 소개 및 동향

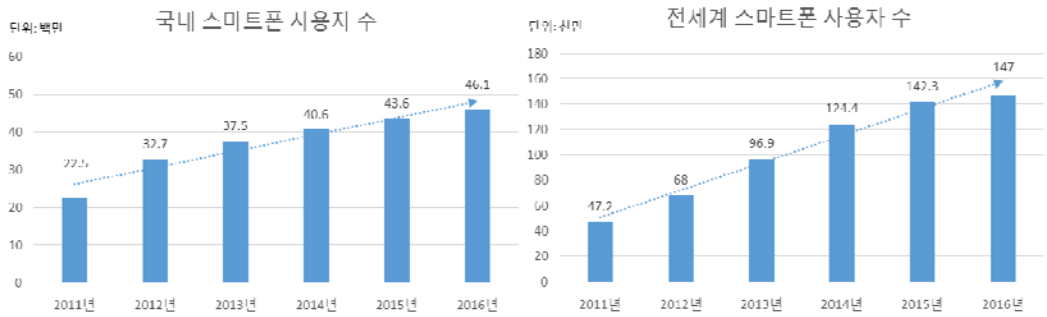
이성훈 김승현* 천은미** 김수형*** 진승헌***
한국전자통신연구원 UST 연구생
한국전자통신연구원 선임연구원 *
한국전자통신연구원 인턴연수생 **
한국전자통신연구원 책임연구원 ***

스마트폰, 태블릿과 같은 개인용 모바일 기기 사용이 급증함에 따라, 기업들은 이들 기기를 업무에 활용하는 BYOD 정책을 도입하여 업무 효율성을 향상시키고 있다. 하지만 기업들은 개인 기기의 보안 취약점으로 인한 기업의 기밀 데이터 유출과 같은 위협을 심각하게 우려하고 있다. 이러한 위협에 대응하기 위한 기술로 EMM, MDM, MAM 등과 같은 모바일 보안 관리 기술이 활성화 되고 있으며, 해외에서는 여러 기업이 저마다의 제품을 개발하고 있다. 본 고에서는 각 모바일 보안 관리 기술을 간략히 소개하고, 해외 기업들이 제공하는 보안 제품을 분석하여 향후 연구 방향을 제시한다.

Ⅰ. 서론

개인용 모바일 기기는 우리 일상에서 보편화된 기기가 되었다. 스마트폰 사용자 수는 [그림 1]과 같이 꾸준히 성장하고 있다. 국내의 경우, 스마트폰 사용자 수는 2016년 10월 약 4,611만 명에 달하고, 전세계의 스마트폰 사용자 수는 2016년 기준 약 14억 7,000만 명에 달한다[1],[2]. 스마트폰 뿐만 아니라 태블릿 등 모바일 기기를 사용하는 국내 이용자는 5,495만 명에 달한다[1]. 이렇게 보편화된 개인용 모바일 기기를 활용한다면 기업의 업무 경쟁력을 향상시킬 수 있다. 기업용 업무 기기를 별도로 소지하고 사용할 경우, 기업의 비용 부담뿐만 아니라 사용자의 휴대성 측면에서 비효율적이다. 하지만 개인용 모바일 기기에서 기업 업무를 수행할 수 있다면, 별도 기기로 인한 비용과 휴대성 문제 없이 기업 업무를 수행할 수 있게 된다. 이렇게 기업 업무에 개인 소유의 모바일 기기 사용을 허용하는 정책을 BYOD(Bring Your Own Device)라고 부르

* 본 내용은 이성훈 UST 연구생(☎ 042-860-6375, sunghoon1130@etri.re.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.



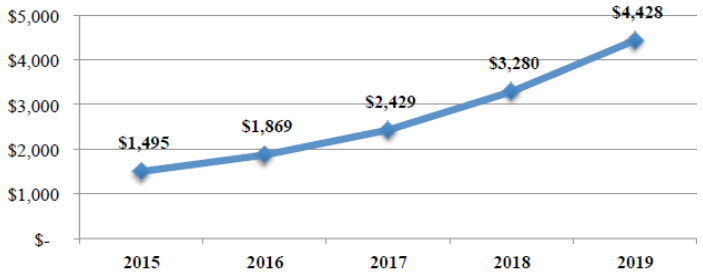
<자료> 국내: 미래창조과학부, 2016, 전세계: Number of smartphones sold to end users worldwide from 2007 to 2015, Statista

[그림 1] 모바일 기기 사용자 수

며, 여러 기업과 공공기관에서 이미 BYOD 정책을 활발히 도입하고 있다[3].

BYOD 도입으로 인해 업무 효율성이 증가하는 반면, 회사의 주요 업무 및 기밀 문서와 같은 중요한 데이터를 사용자의 개인 모바일 기기에 저장하게 됨으로써 모바일 기기 보안이 중요하게 되었다. 모바일 기기 보안을 다룬 한 설문조사에 따르면, 악의적인 와이파이 장치 접속(24%)과 악성코드 다운로드(39%)로 인한 보안 침해를 겪은 사용자가 전체 응답자의 60%에 달했다[4]. 응답자의 37%는 모바일 기기에 보안 침해가 있었는지 조차 확실히 알지 못했다. BYOD 정책을 도입한 회사들은, MDM(모바일 기기 관리) 솔루션을 이용하여 기업 차원에서 보안 침해 사고에 대응하는 움직임을 보여왔다. BYOD 정책을 도입한 회사를 대상으로 한 설문조사에 따르면, MDM 솔루션을 적용한 회사는 약 50%에 달했다. 그리고 나머지 절반의 회사 중에서도 향후 MDM 과 같은 모바일 보안 솔루션 도입을 계획하고 있는 회사가 25%에 달하는 것으로 조사되었다[5].

모바일 보안 관리 기술은 초기에 개인용 모바일 기기 자체를 제어하기 위한 MDM 에서부터



<자료> The Radicati Group, Inc., “Enterprise Mobility Management Market, 2015-2019”, 2015. 5.

[그림 2] 전세계 EMM 시장 규모(2015~2019 년, 백만 달러)

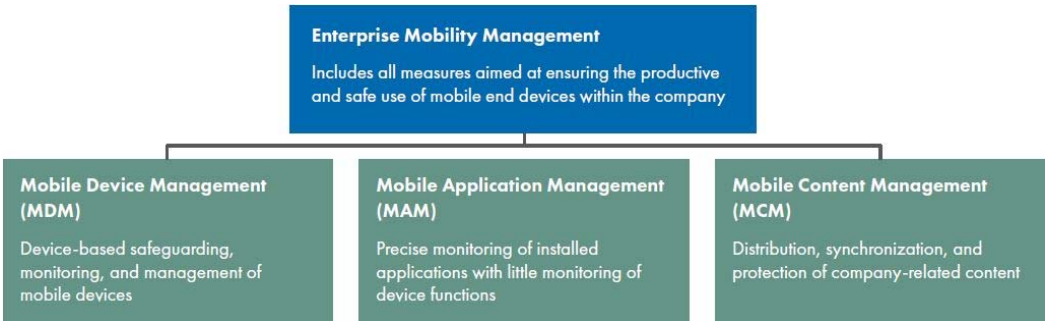
시작하여 기업과 직원들의 다양한 보안 요구사항을 반영하여 기술 범위가 확장되고 있다. MDM 뿐만 아니라, MAM, MCM 등과 같은 요소 기술들을 통합하여 EMM(엔터프라이즈 모빌리티 관리)에 이르기까지 모바일 보안 관리 기술이 활성화되고 있는 추세이다. MDM 과 MAM, MCM 솔루션을 포함한 전세계 EMM 시장 규모는 [그림 2]와 같이 큰 폭으로 성장할 전망이다. IDC 에 따르면 전세계 EMM 시장은 국내외 각각 2019 년까지 연평균 15.7%, 30%씩 성장하여 2019 년 260 억 원, 44 억 달러 규모를 형성할 것으로 전망된다[6],[7].

Ⅱ. 모바일 보안 솔루션

본 장에서는 EMM, MDM, MAM, MCM 등 모바일 보안 솔루션을 제공하는 기술에 대해 소개한다. 각 기술들이 제공하는 기능은 무엇인지, 기능을 제공하기 위해 필요한 기술에는 무엇이 있는지 살펴본다.

1. 모바일 보안 관리 기술 정의

EMM(엔터프라이즈 모빌리티 관리)는 모바일 장치, 무선 네트워크 및 기타 모바일 컴퓨팅 서비스를 관리하는데 중점을 둔 프로세스 및 기술을 의미한다. 개인 모바일 기기를 회사 업무에 사용하기 위해서 필요한 시스템 관리, 안전한 업무 공간 확보를 위한 모바일 솔루션 기능을 제공한다. 즉, 모빌리티 구현 및 지원과 관련된 포괄적인 개념을 말한다. [그림 3]과 같이 EMM 을 구성하는 요소로 MDM, MAM, MCM 기술을 선택적으로 포함하며, 이들 기술을 기업의 보안 정



<자료> Mobile Security The case for Enterprise Mobility Management, FREUDENBERG IT, 2017.

[그림 3] EMM 구성 요소

책에 융화시켜 동작할 수 있는 연동 체계를 지원한다.

MDM(모바일 단말 관리)은 스마트폰이나 태블릿, 휴대용 컴퓨터와 같은 모바일 기기를 관리할 수 있는 기능을 제공하는 기술이다. 모바일 기기에 사용자를 등록하여 사용자 인증 후에 해당 기기를 사용하도록 할 수 있다. 특정 서비스를 활성화시켜 안전하게 모바일 기기를 사용할 수 있는 보안 기능을 제공하거나, 기기 위치 및 자산 추적과 기기 내의 자료 삭제 등의 기능을 제공한다. 하지만, MDM 이 제공하는 보안 기능은 모바일 기기 전체에 적용되기 때문에, 기업의 보안 관리자가 개인의 사생활을 감시하는 프라이버시 문제가 우려된다.

MAM(모바일 애플리케이션 관리)은 MDM 과 유사한 개념이나, 모바일 기기 전체가 아니라 기기에 설치된 일부 특정 앱에만 기업의 보안 정책이 적용된다. MDM 과는 달리, MAM 에서는 기업의 보안 관리자가 업무용 앱만 제어 가능하며, 나머지 앱 사용에 대해서는 사용자의 프라이버시가 보호된다. 예를 들어, 기업은 MAM 을 이용하여 보안 메일, 캘린더, 연락처, 비용 리포트와 같은 기업용 앱을 직원 스마트폰에 배포하고 앱 잠금, 제어, 암호화 기능을 적용할 수 있지만, 기타 다른 앱은 제어하지 않는다.

MCM(모바일 콘텐츠 관리)은 직원들이 기업의 기밀정보와 같은 콘텐츠를 쉽고 안전하게 공유할 수 있는 협업 기능을 제공한다. 파일 동기화 및 공유 기능, 콘텐츠 관리와 시스템 접근 기능 등을 제공한다. 기업은 각 콘텐츠에 대해 직원들의 보안 등급에 따라 접근 권한을 부여하고, 모바일 기기 접근을 관리한다. 또한, 필요한 경우에는 모바일 기기에서 콘텐츠 파일을 임의로 삭제하여 기업의 기밀정보 유출을 방지할 수 있다.

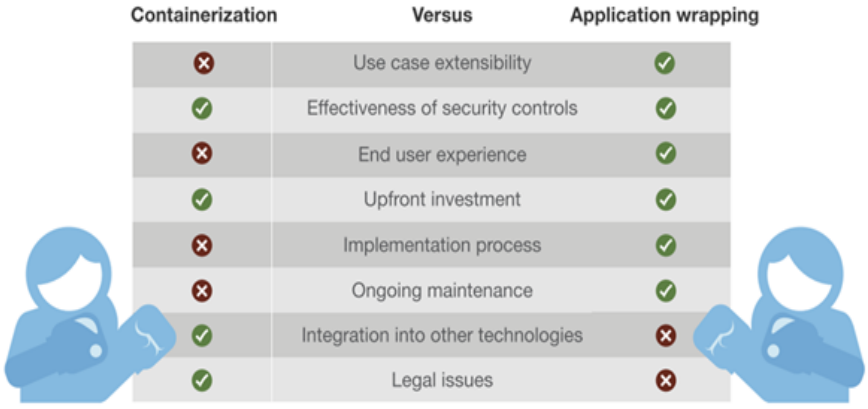
2. EMM 제공을 위한 기반 기술

사용자의 모바일 기기에 EMM 등 기업의 보안 정책을 적용하기 위한 기반 기술로, 컨테이너(Containerization) 기술과 앱래핑(App Wrapping) 기술이 존재한다. 컨테이너 기술은 모바일 기기 저장소의 일정부분을 가상화된 샌드박스(Sandbox)로 만들고, 컨테이너 안에서만 기밀 정보에 접근하거나 업무용 앱을 구동시키는 방식이다. 대표적인 컨테이너 방식으로는 2013 년 초 삼성전자가 미국방부의 보안승인을 받은 기업용 모바일 보안 솔루션인 '녹스(KNOX)'가 있으며, LG 전자에서도 컨테이너 기술을 이용한 'LG 게이트'를 출시했다[8]. 샌드박스 안에서 구동되는 앱은 컨테이너 밖으로 나올 수 없으며, 이메일 등을 통한 외부 공유 시 철저한 인증을 거침으로써 민감한 정보의 외부 유출을 차단한다. 국내 MDM 업체인 지란지교와 라온시큐어 또한 컨테이너

기술을 적용한 모바일 보안 관리 솔루션을 개발하였다[9],[10].

이에 반해, 앱래핑은 단일 앱에 보안 정책을 실행할 수 있는 코드를 직접 삽입하여 앱을 수정하는 방식이다. 바이너리 앱의 소스 코드 없이 앱을 변조하는데, 디컴파일(de-compile)된 앱의 중간 코드(예; 안드로이드 OS 의 경우, smali, jasmin, dex 등)에 회사의 보안 정책을 추가한 이후, 리컴파일(re-compile)하여 안정적으로 앱을 동작시키는 과정이 어렵기 때문에 해당 기술을 보유한 업체가 많지 않다. 국외의 경우, 2012 년에 시만텍에서 앱래핑 기술을 포함한 제품을 출시한 이후로 Citrix, IBM, MobileIron, Mocana 등의 업체들이 제품을 출시하였다[11]. 국내에서는 아직 앱래핑 기술을 보유한 업체가 없고, 국외 제품을 유통하여 출시하는 정도이다[12]. 앱래핑과 컨테이너 기술을 분석한 Forrest 보고서에 따르면, 앱래핑과 컨테이너 기술은 [그림 4]와 같이 각각의 장단점을 가진다[13].

- Use case extensibility: 사용자의 모바일 기기에는 여러 가지 종류의 앱이 설치되어 있으며, 회사 업무 및 보안을 위해 설치된 앱과 사용자가 앱스토어에서 다운로드 받은 앱이 있다. 회사에서 개발된 앱에 보안정책을 적용하는 등의 기능 업데이트를 할 경우, 앱의 원본 소스 코드가 있다면 업데이트와 관련된 코드를 추가로 개발하는 절차가 필요하다. 원본 소스코드를 구할 수 없는 경우, 컨테이너 방식은 기업의 보안 정책을 적용하기 어렵다. 반면에 앱래핑 기술을 이용하면, 앱의 원본 소스코드 유무와 무관하게 바이너리 앱에 직접 코드를 삽입하여 업데이트 기능을 적용할 수 있다. 사용자가 앱스토어에서 다운로드하여 설치한 앱인 경우에도, 컨테이너 방식은 앱의 소스코드 문제로 인해 수정이 어렵지만 앱래핑 방식은 기



<자료> Tyler Shields, “In the mobile security bout of the year, app wrapping beats”, Forrest, July 7, 2014.

[그림 4] 컨테이너 기술과 앱래핑 기술의 비교

업의 보안 정책을 반영할 수 있다.

- Effectiveness of security controls: 기업의 기밀 정보를 열람하는 앱에 효율적으로 기업의 보안 정책을 적용하는 것은 모바일 보안 기술의 가장 중요한 부분이다. 컨테이너 방식은 컨테이너 안에서 실행되는 앱에게 여러 보안 정책을 적용할 수 있다. 마찬가지로, 앱래핑 방식은 원본 소스코드가 없어도 바이너리 앱에 직접 보안 정책 코드를 삽입하기 때문에 폭 넓은 보안 정책을 적용할 수 있다.
- End user experience: 컨테이너 방식의 경우, 사용자가 사용하는 앱은 두 가지 버전(일반 모드에서 작동되는 앱, 샌드박스 안에서 보안정책이 적용된 앱)으로 나뉘어 작동한다. 사용자는 필요에 따라 선택적으로 두 가지 모드 중에 하나의 앱을 구동시켜야만 한다. 하지만 앱래핑 방식의 경우, 회사의 보안 정책이 적용되는 앱은 앱래핑을 거쳐 보안 정책이 자동으로 적용된다. 사용자는 평상시와 마찬가지로 앱을 구동시켜 사용하면 되기 때문에 컨테이너 방식에 비해 더 편리하다.
- Upfront investment: 모바일 앱 보안 기술을 기업 인프라에 성공적으로 적용시키기 위해서는 모바일 기기 및 운영체제 지식 및 보안 기술을 습득한 모바일 보안 전문가가 필요하다. 컨테이너 방식 및 앱래핑 방식 모두 보안을 잘 이해하고 있는 개발자가 필요하다. 그리고 새로운 보안 위협을 지속적으로 확인하고 보안 업데이트를 담당해야 하기 때문에 보안 전문가는 항상 필요한 존재이다.
- Implementation process: 회사의 보안 정책을 모바일 기기에 적용할 때, 보안 정책을 모바일 기기에 적용하는데 소요되는 시간과 비용을 고려해야 한다. 컨테이너 방식은 보안 정책을 적용할 앱을 개발한 회사 또는 모바일 기기 제조사와 협력하여 보안 정책을 적용해야 하기 때문에 많은 시간과 비용이 소모된다. 이에 반해, 앱래핑 빙식은 바이너리 앱만 있으면 보안 정책을 적용할 수 있기 때문에 시간과 비용을 절약할 수 있다.
- Ongoing maintenance: 모바일 앱은 상시 혹은 주기적으로 보안 업데이트를 수행한다. 컨테이너 방식은 보안 업데이트를 적용할 때, 모바일 보안 담당자가 컨테이너에 보안 업데이트를 적용하거나 해당 앱의 원본 소스코드에 직접 보안 정책을 적용해야 한다. 반면에, 앱래핑 방식은 보안 업데이트를 진행할 때, 자동으로 보안 업데이트 정책을 체크하여 해당하는 앱에 업데이트 정책을 적용하기 때문에 유지보수가 용이하다.
- Integration into other technologies: 앱래핑 방식은 보안 정책을 적용하고자 하는 단일 앱에

앱 자체의 기능 제어만을 제공한다. 그렇기 때문에, 통합 앱 스토어 개발, 앱 개발 플랫폼, 신원 관리 등과 같은 보안 이외의 기술을 제공하지 못한다. 반면에, 컨테이너 방식은 인증, 신원 관리, 통합 앱 스토어 개발, 앱 개발 플랫폼 등과 같이 보안뿐만 아니라 보안 이외의 기술들을 제공할 수 있으며, 해당 기술이 없다면 컨테이너 레벨에서 추가도 가능하다.

- Legal issues: 앱래핑 방식은 모바일 앱의 저작권과 애플 iOS 에서 배포된 앱에 대한 약관에 따른 두 가지 법적인 이슈가 있다. 저작권 측면에서, 앱 개발자의 허락 없이 앱을 배포한자 이외에 무단으로 앱을 수정하는 것은 불법으로 간주될 수 있다. 또한, 애플 앱스토어에서 배포된 앱을 대상으로 어떤 방식으로도 수정하는 것은 애플 앱 약관을 위반하는 행위이다. 반면에, 컨테이너 방식은 앱 개발자 및 기기 제조사와 협력하여 보안 정책을 적용하기 때문에 법적 이슈 없이 사용할 수 있다.

앞서 살펴본 각각의 관점에서 컨테이너와 앱래핑 방식을 비교하면, 앱래핑 방식은 바이너리 앱을 직접 수정하여 보안 정책을 적용하기 때문에, 법적인 이슈가 존재하고 보안 이외의 기술을 제공하지 못한다는 단점이 있다. 하지만, 앱래핑 방식은 바이너리 앱에 직접 보안 정책을 적용함으로써 시간, 비용, 유지 관리에서 컨테이너 방식에 비해 우위를 보인다. 각 방식의 장단점을 고려하여 기업의 보안 정책을 적용하는 앱과 모바일 앱 보안에 필요한 기술에 따라 앱래핑과 컨테이너 방식 중에 적합한 기술을 이용해야 한다.

Ⅲ. 모바일 보안 관리 제품 비교

모바일 보안 관리 제품은 국내외 다수의 회사들로부터 제공되고 있다. 해외의 경우, Apperian, Citrix, IBM, MobileIron, Mocana, Symantec, VMware 등의 회사에서 솔루션을 제공하고 있다. 각 회사 제품들이 공통적으로 제공하는 기능과 차별적으로 제공하는 기능은 [표 1]과 같으며, 현재까지 출시된 제품들이 공통적으로 제공하는 기능은 다음과 같다.

- 앱 업데이트 수행: 추가적인 보안 정책이 있거나 수정이 필요한 경우, 관리자가 정해진 시간 혹은 수시로 업데이트를 제공한다.
- 인증 및 Single Sign-On(SSO): 앱 실행 시에 기업의 보안 정책 수준에 맞는 인증을 요청하여 인증된 사용자에 한해 앱을 사용할 수 있다. 한 번의 인증으로 보안 정책이 적용된 다른 앱도 추가 인증 요청 없이 사용 가능한 SSO 기능을 제공한다.

[표 1] EMM 솔루션 비교

회사	Apperian	Citrix	IBM	MobileIron	Mocana	Symantec	VMware
제품명	Apperian	Xenmobile	MaaS360	MobileIron	Mobile App Protection	Mobility Suite	AirWatch
지원 OS	A, I	A, I, W	A, I, W, M	A, I, W	A, I	A, I, B	A, I, W, M, B, S
앱 배포	G, A	G, A, W	G, A, W	G, A, W	G, A	G, A	G, A, W
업데이트	○	○	○	○	×	○	○
인증&SSO	○	○	○	○	○	○	○
루팅 탐지	○	○	○	○	○	○	○
블랙/화이트 리스트	○	○	○	○	×	○	○
DLP	○	○	○	○	○	○	○
암호화	○	○	○	○	○	○	○
저장 정책	○	○	○	○	○	○	○
VPN	○	○	○	○	○	○	○
원격 관리	○	○	○	○	×	○	○

지원 OS: Android(A), iOS(I), Windows(W), MAC(M), Blackberry(B), Symbian(S)
앱 배포: Google PlayStore(G), Apple AppStore(A), WindowsStore(W)
<자료> Ken Hess, "5 Mobile application management features that matter", tom's IT PRO, 2014. 6. 13.

- 데이터 암호화: 유출 방지가 필요한 기밀 문서 및 파일에 대해 데이터 암호화를 지원한다. 인증된 사용자만 기밀 문서 및 파일의 내용을 확인할 수 있으며, 기밀 문서가 외부에 유출되어도 정보 노출을 방지한다.
- 데이터 저장 정책 제어: 사용자 기기에 저장되는 데이터 중에서 기밀 문서나 중요한 데이터 파일을 암호화 하거나, 삭제하여 외부로 유출되지 않도록 기업의 보안 정책을 설정하고 관리한다.
- 데이터 유출 방지(DLP): 앱 상에서 데이터의 복사/붙여넣기 등의 기능을 제어하거나 이메일 등을 통해 문서를 외부로 유출하는 기능을 차단하여 기밀 정보를 보호한다.
- 탈옥/루팅 탐지: 사용자 기기가 탈옥 혹은 루팅되었을 경우, 기밀 정보에 접근하는 업무용 앱 사용을 제한하여 중요한 데이터의 유출을 방지한다.
- 앱 블랙/화이트 리스트: 앱 별로 위험도를 분석하여 화이트리스트와 블랙리스트를 관리하고, 특정 앱의 사용자 기기 설치 가능 여부를 구분한다.
- 안전한 통신(App-level VPN): 기업 외부에서 모바일 오피스 앱에 접속하거나 기밀 문서를 메일로 전송할 경우에 VPN 을 통해 안전한 통신을 제공한다.

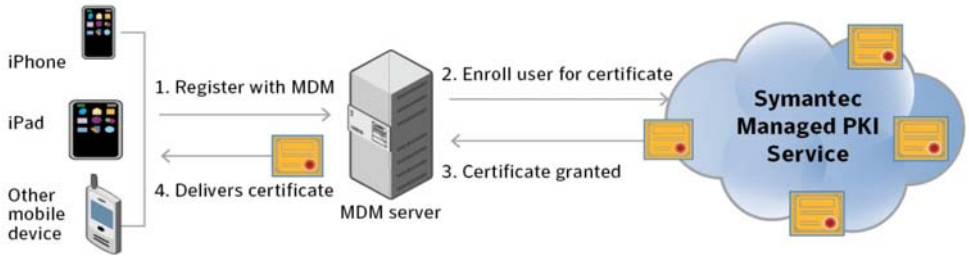
<자료> APPERIAN, "product introduction-Dynamics Policies", 2016. 10.

[그림 5] 동적 정책 엔진 GUI

위의 공통기능 이외에도, 각 회사 제품별로 독자적인 기술을 제공한다. Apperian 사의 제품인 경우, 동적 정책 엔진(Dynamic Policy Engine) 기능을 제공하여 앱의 리컴파일이나 코드 수정 없이 원하는 정책을 언제든지 앱에 적용할 수 있다. [그림 5]와 같이 간단한 체크박스 GUI 형태의 관리화면을 통해, 관리자는 앱에 적용할 보안 정책을 체크하여 선택적으로 적용이 가능하다[15].

Citrix 사의 Xenmobile 제품은 강화된 콘텐츠 관리 및 데이터 보호 솔루션을 제공한다[16]. 로컬 기기에서 작성된 문서를 자동으로 안전한 클라우드 서버에 업로드하여 인증된 직원들 간에 편리하게 문서를 공유할 수 있게 한다. 또한, 마이크로소프트 워드, 엑셀, 파워포인트, PDF 등 여러 문서 편집 기능을 지원하는 자체 통합 문서 편집기를 제공한다. 영국의 대영 도서관을 비롯하여 LeapFrog 사, Sabre Pacific 사들이 Citrix 솔루션을 적용하고 있다.

IBM 사의 MaaS360 제품은 자동화된 위협 탐지 및 위치 기반 정책을 제공한다. 네트워크 연결 또는 기기의 물리적 위치 변화에 따라 다른 동적인 정책 설정이 가능하다[17]. 예를 들어, 사용자 단말기기가 기업 내부에 있는지 외부에 있는지를 확인하여 자동으로 기업의 보안 정책을 적용 또는 미적용시키기 때문에 사용자에게 편리함을 제공할 수 있다. 또한, 사용자의 모바일 기기를 상시 모니터링하여 보안 규칙의 위반 사항이 감지되면 사용자 알림 및 장치 장금 혹은 위험요소 제거 기능을 적용한다. IBM 사의 제품은 Cisco 사 모바일 협업 관리 서비스(MCMS) 및 BlackBerry 사의 SecuTablet 에 적용되고 있다.



<자료> Symantec, "Why digital certificates are essential for managing mobile devices", 2012. 10.

[그림 6] 시만텍 통합 PKI 서비스

Symantec 사의 MobileSuite 는 앱래핑 기술을 제공하여 앱의 원본 소스코드 없이 보안 정책이 적용 가능하다. 보안 요소가 적용되지 않은 업무용 앱에 사용자 인증, 데이터 암호화, 문서 공유, 복사/붙여넣기 제어 등의 기능을 제공한다. 또한, Symantec 이 관리하는 인증서를 [그림 6]과 같은 절차로 배포하여 사용자 모바일 기기에서 VPN, Wi-Fi, Exchange ActiveSync 서비스를 간편하고 안전하게 이용할 수 있도록 지원한다. 모바일 보안 관리자는 각 사용자별로 인증서를 직접 관리하지 않고, 통합된 인증서 관리 시스템에서 일괄적으로 사용자용 인증서를 배포 및 관리함으로써 효율적으로 단말 기기 관리를 수행할 수 있다[18].

VMware 사의 AirWatch 제품은 Google 플레이스토어나 iOS 의 앱스토어와 같은 공개 앱스토어와 연동하여 앱 배포가 가능하다. 관리자는 관리자 메뉴를 통해서 공개 앱 스토어에서 앱을 검색하고, 보안 정책을 적용하여 앱을 배포할 수 있다[19]. 또한, 여러 보안 업체와 모바일 보안 협약(Mobile Security Alliance, MSA)을 맺어서, 기업 내에 모바일 기기의 보안을 위협하는 취약점을 실시간으로 공유하여 [그림 7]과 같이 모바일 기기 혹은 모바일 앱에 취약점 패치를 적용하는 신속한 보안 업데이트를 제공한다. Delta Airlines, Wallgreen, National Bank of CANADA, Lowe's, Bandalux 사들이 AirWatch 솔루션을 이용하고 있다.

<자료> VMware, "Unifying Threat Security with Enterprise Mobility Management", 2016. 10. 16.

[그림 7] AirWatch EMM 을 위한 실시간 보안 취약성 업데이트 흐름도

Ⅳ. 결론 및 시사점

모바일 기기가 일반화 됨에 따라 기업에서는 개인용 모바일 기기를 활용한 BYOD 정책을 도입하여 업무 효율성 향상을 기대하고 있다. 하지만 기밀 데이터 유출 보안 위협이 존재함에 따라, 회사의 중요한 정보를 안전하게 보호하는 모바일 보안 솔루션이 중요시되고 있다. 이에 본고에서는 MDM, MAM, EMM 등 모바일 보안 솔루션 기술을 정리하고 모바일 보안 솔루션 기술을 제공하기 위한 방법으로 앱래핑과 컨테이너 기술을 비교·분석하였다. 또한, 해외 관련 기업의 모바일 보안 솔루션이 제공하는 기능을 분석하였다. 향후 모바일 기기를 활용한 기업 업무가 증가함에 따라 EMM 기술 등 모바일 보안 솔루션 시장이 더욱 활성화되고 기술적 부분에서 도 더욱 고도화 될 것으로 전망한다.

[참고문헌]

[1] 박단일, “2016년 10월 무선통신서비스 가입자 현황”, 미래창조과학부, 2016. 11. 30.
[2] Statista, “Number of smartphones sold to end users worldwide from 2007 to 2015(in million units)”, accessed data: 2017. 2. 20.
[3] 강정구, “Beyond BYOD, 기업 소유 강화로 모바일 패러다임 변화 시작”, 전자신문, 2016. 4. 13.
[4] Matt Hamblen, “기업 21%, 사내 모바일 기기 관련 보안 사고 있었다”, CIO KOREA, 2016. 3. 30.
[5] “Mobile security 2015 study”, computerwoche and TecChannel, 9, 2015.
[6] “Enterprise Mobility Management Market, 2015-2019”, The Radicati Group, Inc., 2015. 5.
[7] 김현주, “국내 EMM 소프트웨어 시장 2019년까지 연평균 15.7% 성장 전망”, 한국IDC, 2016. 1. 12.
[8] 김선애, “MDM, BYOD 보안 위해 모바일 보안 플랫폼으로 진화해야”, 데이터넷, 2014. 1. 9.
[9] 최민지, “지란지교시큐리티, 모바일 컨테이너 플랫폼 선봬”, 디지털데일리, 2016. 6. 21.
[10] 황치규, “라온시큐어도 삼성 녹스 기반 MDM 사업 참여”, ZDNet Korea, 2014. 5. 28.
[11] Minh Phan, “New Release of Symantec App Center”, Symantec, 2012. 10. 22.
[12] 노동균, “엑스퍼넷, 모바일아이언 EMM 솔루션 국내 총판 계약 체결”, IT조선, 2016. 6. 30.
[13] Tyler Shields, “In the mobile security bout of the year, App wrapping beats containerization on points”, FORRESTER, 2014. 7. 7.
[14] Ken Hess, “5 Mobile application management features that matter”, tom’s IT PRO, 2014. 6. 13.
[15] https://www.apperian.com/mobile-application-management/mobile-app-wrapping/
[16] Citrix XenMobile vs. AirWatch: Five reasons AirWatch can’t match XenMobile for empowering business mobility, Citrix, 2014.
[17] Peter Sterk, “Enterprise mobility management smackdown”, PQR, 2014. 10.
[18] “Why digital certificates are essential for managing mobile devices”, Symantec, 2012. 10.
[19] 임관수, “엔터프라이즈 모빌리티 솔루션 도입시 고려사항”, VMware, 2016. 6. 16.